UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF: One Apple iPhone Model A1453, IMEI: 35202606520062, belonging to Logan Gienger and currently in the possession of ICAC	CASE NUMBER: 5:18-mj-154 **AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION**

State of South Dakota)
) ss
County of Pennington)

I, John Barnes, Special Agent (SA) with South Dakota Division of Criminal Investigations (DCI), being duly sworn, state as follows:

1. I am a Special Agent with the South Dakota Division of Criminal Investigation and have been so employed since August of 2014. During that time, I have attended the South Dakota Division of Criminal Investigation 13-week basic law enforcement-training academy and then completed the 10-week field training. I have also attended the one-week DCI crime scene training in Pierre, SD, the DEA Clandestine Laboratory Investigation/Safety Certification Program in Quantico, VA, the MCTC Science Based Drug Education course, the National Guard Counterdrug Aviation Policy course, the NTOA Advanced Crisis Negotiations course, the Basic Data Recovery and Acquisition course, and the Intermediate Data Recovery and Analysis Course. I attended Black Hills State University and graduated with a Bachelor's Degree in Business Administration with a specialization in Accounting. Currently, I am assigned to the ICAC Task Force (Internet Crimes against Children). The investigations worked by this unit include child pornography, solicitation of minors, sexual exploitation of minors,

disseminating harmful materials to minors, and human trafficking. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include 18 U.S.C. § 2422(b), enticement of a minor using the internet. During my law enforcement-career, I have become familiar with the *modus operandi* of persons who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who exploit children on the internet.

2. During my law enforcement career, I have become familiar with the *modus operandi* of persons involved in enticement of a minor using the internet in violation of federal law. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally attempt to meet with children in order to engage in criminal sex acts.

3. The information set forth below is based upon my knowledge of an investigation conducted by the South Dakota Internet Crimes Against Children Taskforce (ICAC) and the investigation of other law enforcement agents and officers including, but not limited to, South Dakota Division of Criminal Investigation (DCI), Homeland Security Investigations (HSI), the Rapid City Police Department, and the Pennington County Sheriff's Office. I have not included every fact obtained pursuant to this investigation, but have set forth those facts that I believe are essential to establish the necessary probable cause for the

criminal complaint. I have not omitted any material fact relevant to the consideration of probable cause for the location and items described below.

4. I have been informed that 18 U.S.C. § 2422(b), Enticement of a Minor Using the Internet, makes it a crime for a person to use the internet or any other means, which affects interstate commerce, attempt to knowingly persuade, induce, entice, and coerce a person who has not attained the age of 18 years to be caused to engage in a criminal sex act.

5. Your affiant respectfully submits that there is probable cause to believe that Logan Gienger committed the crime enticement of a minor using the internet in violation of 18 U.S.C. § 2422(b) utilizing the subject device: One Apple iPhone Model A1453, IMEI: 35202606520062, belonging to Logan Gienger and currently in the possession of ICAC.

ITEMS TO BE SEARCHED FOR AND SEIZED:

6. Any evidence of the defendant's efforts to persuade, induce, entice, and coerce a person who has not attained the age of 18 years to be caused to engage in a criminal sex act.

7. Any visual depiction of minors engaged in sexual activity, to include but not limited to images and videos.

8. Any written correspondence with minor children or adults describing any sexual acts with minors in any form, but not limited to emails and text messages.

9. Any other images or video files of criminal activity involving

children.

10. The undersigned respectfully requests that a search warrant be issued to permit a search of one Apple iPhone Model A1453, IMEI: 35202606520062, belonging to Logan Gienger and currently in the possession of ICAC, hereinafter referred to also as SUBJECT DEVICE.

11. I submit that there is probable cause to search for evidence, fruits, and instrumentalities of 18 U.S.C. § 2422(b), Attempted Coercion and Enticement of a Minor, prohibits using the mail or any facility of interstate of foreign commerce, to knowingly persuade, induce, entice, or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

DEFINITIONS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. *Child Erotica*: as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. *Child pornography*: as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. *Cloud-based storage service*: as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. *Computer:* The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

f. *Computer Hardware:* The term "computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. *Computer-related documentation*: as used herein, consists of written, recorded, printed, or electronically stored material which explains or

illustrates how to configure or use computer hardware, computer software, or other related items.

h. *Computer Passwords and Data Security Devices:* The term "computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. *Computer-Related Documentation:* The term "computer-related documentation" means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. *Computer Software:* The term "computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in

electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. *Electronic Communication Service* ("ESP"): as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

m. *File Transfer Protocol* ("FTP"): as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. *Internet:* The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

o. *Internet Connection:* The term "Internet connection" means a connection required for access to the Internet. The connection would generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

p. *Minor:* The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

q. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. *Remote Computing Service* ("RCS"): as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. *Short Message Service* ("SMS"): as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

t. *Storage Medium:* The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u. *Visual Depictions:* "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

v. *Wireless Network:* The term "wireless network" means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

PROBABLE CAUSE

13. On 9/18/18, I was involved in an undercover law enforcement operation in Rapid City, SD. This operation was conducted by members of the South Dakota Internet Crimes Against Children (ICAC) Task Force which includes law enforcement officers from the Rapid City Police Department, the Pennington County Sheriff's Office, and the South Dakota DCI as well as agents from Homeland Security Investigations. During this particular operation I was acting in an undercover capacity as a "pimp" in which I was offering a minor for prostitution.

14. On 8/7/18, Homeland Security Investigation (HSI) Special Agent Scott Beagle put up an ad on the website CityXguide.com. SA Beagle was acting in an undercover capacity during an operation held during the 2018 Sturgis Motorcycle Rally. The ad had the following information:

Title: "new and fresh girl in rapid city" -19 (Rapid City)

Category: Female Escorts

Name: amber

Phone: Undercover (UC) phone number

Email: UC Email

Location: Rapid City

Age 19:

Last updated: Aug 7, 2018, 18:49 PST

The ad also stated the following: "text me for more info. I don't wanna get booted from here. let me know u saw ad on cityxguide" and included an image of an age regressed photo of an adult female who is affiliated with law enforcement.

15. The ad was posted on CityXGuide.com and under the Category "Home-United States-South Dakota-Rapid City."

16. On 9/16/18, SA Beagle contacted me and informed me that he had an individual that has responded to the ad that he had posted on CityXGuide during the 2018 Sturgis Motorcycle Rally. He informed me that this individual had contacted him from the phone number (605)431-4012 and they had communicated through text messages. The person using the number was later identified as Logan Matthew Gienger (DOB x/xx/1994). The communications between SA Beagle and Gienger started on Friday 9/14/18 and continued until Sunday 9/16/18.

17. In his undercover persona, HSI Beagle was acting as a 14 year-old female prostitute. During this conversation, they discussed that the female prostitute was 14 years old and that Logan would have to contact her pimp. Logan told the 14 year-old female that he was looking for "Oral and vag for hr, what will you do?"

18. On Sunday 9/16/18, HSI Beagle in his undercover persona gave Logan my undercover phone number to continue the conversation in an undercover capacity as a pimp. HSI Beagle provided my UC phone number and said "Say u wanna meet April or he won't answer. Ttyl."

19. That evening, on 9/16/18 at 8:05PM, I received a text message from Logan (605-431-4012), in which he wrote "I would like to meet April." During this conversation I asked Logan how old did the female tell him she was and he responded "fourteen." He was asked what he was looking for and he told me he was looking for "bareback traditional, greek, and oral with swallow." Based on my training and experience I understand that bareback is a term used for sex without a condom. Also, "greek" is a term used for anal sex.

20. I sent Logan the following message, "okay cool, just so were clear, you are cool with her being 14yrs old? I don't want any surprises.". I then sent the following message, "I deleted our messages when i was cleanin (sic) out my phone. just make sure your cool with her age." Logan responded with "Yeah I'm ok with that lol." Ultimately Logan Gienger agreed to pay $80.00 for a half hour of bareback sex to include oral sex. Logan was told that the meeting location was at the Best Western Ramkota Hotel in Rapid City, South Dakota, on the north side.

21. An undercover officer parked an undercover vehicle on the north side of the Best Western Ramkota hotel. At approx. 2:38PM, Logan appeared at the Ramkota as scheduled and was arrested after he got into an undercover officer's vehicle. He had provided the UC officer the $80.00 previously discussed. Logan was also in possession of the SUBJECT DEVICE, an Apple iPhone. I was later informed that Logan also had a plastic bag of marijuana in his vehicle.

22. A subsequent interview was conducted with Logan, during which he confirmed his phone number that had been used in the conversations. He confirmed that he was the individual that had responded to the ad that was posted on the "CityXGuide" website. He confirmed that he had agreed to pay $80.00 for a half hour of bareback sex to include oral sex with the 14 year-old juvenile prostitute. Logan confirmed that he knew this was illegal.

23. I am aware that "CityXguide" operates solely on the internet and is therefore in and affecting interstate commerce.

=Your affiant wishes to draw the Court's attention to the following facts regarding inferences from the above-mentioned facts that are based upon my knowledge, training and experience:

24. I am aware that often times, even persons who know they are under investigation for internet crimes, will not discontinue their criminal conduct. Sometimes this is because they believe they will outsmart the investigators through their computer knowledge, or because they are addicted to their criminal conduct or if they believe they have gotten away with their prior internet crimes due to the passage of time since the inception of the investigation.

25. Through my training and experience I am aware people involved in the online exploitation of children, especially those who are computer-savvy, may use cloud services and may have multiple devices which access the cloud storage device. This may be accomplished utilizing a cell phone, tablet, computer, or other device which has access to the internet.

26. I know that individuals who are involved in the online exploitation of children will often store evidence of their exploitation on their computer system. I also know that when an individual utilizes multiple storage systems, there is often evidence of child exploitation stored in multiple locations.

27. I know that electronic and/or written communication may exist on the computer system, demonstrating the access to an app or website used for the exploitation of minors. I know that exchanging images during chats, such as photos of the offender sent to the minor or vice versa, frequently causes the displayed images to be saved to the hard drive of the computer or in the "images" or "photos" file on a smart phone or tablet. The device may store the images even if the user believes them to be deleted.

28. I know people involved in the online exploitation of children typically associate online with other people with similar deviant sexual interests in children. Accordingly, there is commonly remnants of communications between the offender and other offenders.

29. I know that people who use personal computers in their homes tend to retain their personal files and data for extended periods of time; months or even years. Due to a personal computer's unique ability to store large amounts of data for extended periods of time without consuming much additional physical space; people tend to retain this data. Affiant knows this to be true regardless of whether or not a person has traded-in or "upgraded" to a new personal computer. Personal computer users routinely transfer most of their data onto

their new computers when making an upgrade. This data transfer is often done by saving files from the old computer to media sources (CD's or floppy disks, etc.) and then saving them to the new hard drive. Any evidence of online exploitation of minors is as likely as other data to be transferred to a person's new, replacement or upgraded computer system.

30. I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools.

31. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the

instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

32. Based on my training and experience, I know that data can be received by use of a home computer and transferred to other electronic devices, such as a cell phone. I also know that data or images can be received by use of a cell phone and transferred to a home computer.

33. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices

require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

34. Your affiant is aware that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies for a

standard computer can take several business days. Complex systems or recover tasks can require much longer time-periods. Due to the back load of computers waiting to be examined and the limited number of trained examiners, any item seized pursuant to this warrant may be examined outside the regular 14-day time period. Further:

a. I know that searching and seizing information from computers often requires investigators to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following: The volume of data stored on many computers and other electronic storage media is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site.

b. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence

and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction, a controlled environment is essential to ensure its complete and accurate analysis.

LIMIT ON SCOPE OF SEARCH

35. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

36. Based on the foregoing, your affiant respectfully requests a warrant for the search of the following three electronic device: one Apple iPhone Model A1453, IMEI: 35202606520062, belonging to Logan Gienger and currently in the possession of ICAC.

Further your affiant saith not.

Dated: 10/13/18

Special Agent John W. Barnes
South Dakota DCI
South Dakota ICAC

SUBSCRIBED and SWORN to
dlw in my presence
_____ by reliable electronic means

this 15th day of October, 2018.

DANETA WOLLMANN, U.S. MAGISTRATE JUDGE

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

- One Apple iPhone Model A1453, IMEI: 352026065200 62, belonging to Logan Gienger and currently in the possession of ICAC

ATTACHMENT B
Information to be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2422(b), enticement or attempted enticement of a minor using the internet and 18 U.S.C. § 1591, commercial sex trafficking of a minor:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTERS"):
    a. evidence of who used, owned, or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
    e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
    f. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;
    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTERS;
    h. evidence of the times the COMPUTERS were used;
    i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTERS;

j. documentation and manuals that may be necessary to access the COMPUTERS or to conduct forensic examinations of the COMPUTERS;
k. records of or information about Internet Protocol addresses used by the COMPUTERS;
l. records of or information about the COMPUTERS' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including
   a. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
   b. Records and information relating to sexual exploitation of children, including correspondence and communications between Whisper app users.
6. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
7. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones (cell phones), tablets, certain gaming devices, server computers, and network hardware.
8. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include but are not limited to internal and external hard drives, SD cards, storage disks (CDs and DVDs), flash memory, other magnetic or optical media and "cloud" storage by any provider.